REMARKS/ARGUMENTS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 USC § 103. Thus, the Applicants believe that the pending claim is now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Ms. Alberta A. Vitale, Esq. at (203) 469-8097 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Status of pending claims

Claims 1, 2, 16, 17 and 26 are currently amended. No claims have been added or canceled.

Claim amendments

The claims have been amended to clarify the nature of the present invention. In particular, each of independent claims 1, 16 and 26, has been amended to make clear that the step of identifying data relating to one or more relevant server protocols involves identifying such data "from the received data." In addition, the final clause of each of these claims has been amended to make it

clear that the device determined to be the server device is that which has the highest data volume for communications in which it is involved (i.e., in which it is the source or destination device) and "in which at least a threshold number of other devices are involved."

The term "management data" previously used in dependent claims 2 and 17, has been replaced by "received data."

In view of the amendments presented above the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 USC § 103(a). Thus, the Applicants believe that all of these claims are now in allowable form.

Rejections under 35 USC § 103

A. Claims 1-6, and 10-15

The Office Action, at paragraph 3, has rejected method claims 1-6, and 10-15 under 35 USC § 103(a) as being unpatentable over the Kosbab patent (United States patent 5,917,808 issued to Bruce James Kosbab on June 29, 1999 (hereinafter Kosbab '808)) in view of the Dieboll patent (United States patent 5,886,643 issued to Robert S. Dieboll, et al on March 23, 1999 (hereinafter Dieboll '643)) and further in view of the McKee patent (United States patent 5,712,981 issued to Neil H. McKee, et al on January 27, 1998 (hereinafter McKee '981)).

B. Claims 16-21, 24-25 and 26-28

The Office Action, has further rejected corresponding computer program claims 16-21 and 24-25 (paragraph 4) and apparatus claims 26-28 (paragraph 5) under 35 USC § 103(a) as being unpatentable over Kosbab '808 in view of Dieboll '643 and further in view of McKee '981.

C. Claims 7-9 and 22-23

The Office Action, at paragraph 5, has further rejected dependent claims 7-9 and 22-23 under 35 USC § 103(a) as being unpatentable over Kosbab '808 in view of Dieboll '643 in further in view of McKee '981. in further in view of the Maddalozzo patent (United States patent 5,974,460 issued to John J. Maddalozzo Jr., et al on October 26, 1999 (hereinafter Maddalozzo '460)).

Assuming arguendo that the amendments made herein do not leave the claims in allowable form, Applicants believe that the remarks set forth below overcome the obviousness rejections.

In the interest of prosecution efficiency, Applicant will discuss the rejections in the context of independent claims 1, 16 and 26. Applicants respectfully disagree with the rejections set forth in the Office Action. In particular, Applicants submit that it would not have been obvious to the skilled person, at the date of the

present invention, to arrive at the present invention as defined in each of claims 1, 16 and 26, from the teachings of Kosbab '808, Dieboll '643 and McKee '981 individually or in combinations as applied.

Kosbab '808 discloses a portable test instrument that tests a LAN network by passively monitoring data frames, for the identification of device types, including the identification of servers. However, Kosbab '808 does not disclose identifying data relating to one or more relevant server protocols. Rather, Kosbab '808 works by identifying server frame types. In particular, Kosbab '808 implemenets live frame capture and looks to see whether a frame is a reply frame for a particular server (see description of step 224 in column 8). For this, it is necessary to determine the source port number indicated in the frame. As is well known in the art, certain types of server listen on a fixed port number. For example, an HTTP server listens on port 80. Thus, if a reply frame has a source port number of 80, then the network device at the source address is an HTTP server.

Thus, Kosbab '808 does not disclose "identifying, from the received data, data relating to one or more relevant server *protocols*." (Claims 1, 16 and 26). Rather it identifies server *frame types*, which involves identifying a different type of data in a frame, in particular more detailed data that can be acquired by live packet capture. The processing involved in determining

server protocols as opposed to identifying server frame types is therefore quite different.

Applicants further note that Kosbab '808 is not comparing *"protocols"* (claims 1, 16, 26) but rather frame *messages/types.* This is clear from the Kosbab '808, at col. 3, lines 5-24, which states:

> The frames being sent may contain information that may be uniquely associated with specific types of network devices such as servers, routers, printers. For example, frames containing router information protocol (RIP) messages may be assumed to be generated by one or more routers. . . . Frames containing RIP messages, for example, may thus be used to enter the device type as router in the station database for each entry associated with the network address.

Kasbob '808 further provides examples of messages/frame types that use the RIP protocol, including the following examples: "TCP IP multicast RIP (Routing Information Protocol) reply," (col. 7, line 37 and "IPX RIP reply" col. 7, line 52). Thus, it can be understood that RIP reply messages are responses to RIP requests which can only originate from a router. This further supports Applicants point that Kosbab '808 is not comparing "protocols" (see Applicants' Claims 1, 16 and 26). Rather Kosbab is comparing frame messages/types. Thus Applicants' claimed invention and Kosbab '808 are clearly different.

Dieboll '643 discloses a Network Management System (NMS), which retrieves SNMP MIB data collected by probes on a monitored network. This data is not frame data, but rather more limited statistical data (i.e., static data) collected by probes that monitor data frames in accordance with SNMP. (see col. 5). "The NMS periodically polls . . . the probes to retrieve the data, and the data is stored in an external database as records, each record associated with a conversation between a source-destination pair." (col. 5, lines 29-34, emphasis added). Due to the use of multiple probes at different locations on the network, a conversation may be detected by more than one probe, leading to the duplication of data. To avoid processing the duplicated data, when generating reports for a particular source-destination pair, the NMS identifies the probe that has detected all of the conversations between the two devices of interest. This is the probe that has the highest total packet count for the source-destination pair. The records for this probe are then tagged for use in report generation.

Dieboll '643 states that the NMS can generate reports upon request by the network manager "to identify all of the servers that a particular node is talking to." (col. 5, lines 26-27, emphasis added). However, there is no disclosure as to *how* servers are differentiated from other network devices such as clients. This suggests that the NMS already knows which devices are acting as servers, for instance based on manually input data, as is conventional in the art, and then identifies the records

for conversations involving the particular node and any of the known server devices. Irrespective of this, it is clear from Dieboll '643 that this type of report generation is not related to the identification of the probe with the highest packet count for a particular source-destination pair, as the Office Action appears to suggest. The identification of the probe with the highest packet count is based solely on information in a single record, and is used for report generation for that source-destination pair, as discussed above. It cannot be used to identify all of the servers that a particular node is talking to, since it only relates to the conversations between two nodes.

Dieboll '643 also states that the NMS can generate reports upon request by the network manager "to identify the protocols that are being used over a particular line." (col. 5, lines 28-29). However, this is a separate report request from the identification of servers used by a particular node, and the information provided by such a report is used by the network manager for a different purpose. There is no teaching that any of the reports to the network manager (described at col. 5, lines 25-29) are interrelated, or that the NMS uses the information generated in one report to generate other reports. Specifically, there is no teaching or suggestion that the identification of servers of a particular node is based on information about the protocols used on a particular line on the network.

McKee '981 discloses an "Extract-Servers program 10" which analyses traffic data and determines a list of global servers and local servers. (see col. 7). McKee '981 makes it clear that the "Extract-Servers program" determines which nodes are global servers and which nodes are local servers "simply on the basis of traffic linkage magnitudes." (col. 7, lines 19-22). Traffic linkage in the context of both "global servers" (col. 8, lines 10-25) and "local servers" (col. 9, lines 3-9) is defined as "a count of [the number of] peer nodes," or alternatively, the traffic count (col. 9, lines 3-6). A device is identified as a candidate global server according to the proportion of communications with all the logical segments of the network, whereas a device is identified as a candidate local server according to the proportion of communications with the logical segment it is on. These proportions differentiate local servers from global servers. From the candidate global servers, the device identified as a global server is the candidate device with the highest peer node count and/or data volume count. (col. 8, lines 32-41). Similarly, from the candidate local servers, the device identified as a local server is the candidate device with the highest peer node count and/or data volume count. (col. 9, lines 10-15).

McKee '981 neither explicitly nor implicitly suggests comparison of the traffic linkage with a pre-determined threshold number of peer nodes. On the contrary, the McKee '981 "Extract-Servers program" simply makes the decision that the candidate device which

communicates with the most other devices must be acting as a server. McKee '981 has no explicit or implicit suggestion of a *threshold* for the traffic linkage (peer node count or data volume) in order for a device to be determined to be a server (global or local).

Thus, Kosbab '808, Dieboll '643 and McKee '981 individually or in the combination cited in the obviousness rejections disclose the present invention including the following novel clauses recited in independent claims 1, 16 and 26:

> [I]dentifying, from the received data, data relating to one or more relevant server protocols, and . . . using the identified data, determining as a server device, the device which has the highest data volume for communications in which it is the source or destination device and in which at least a threshold number of other devices are involved. (Emphasis added).

Specifically, none of the prior art documents identify data relating to relevant server protocols, and from that data, determine a device as a server if it has both (i) the highest data volume, and (ii) at least a threshold peer node count.

Additionally, there is no motivation to combine the teaching of Kosbab '808 with either of the teachings of Dieboll '643 or McKee '981.

In particular, Kosbab '808 discloses a technique for identifying servers by using a test instrument that is temporarily connected to a network to capture live data frames. The technique Kosbab '808 employs is accurate because it captures complete data frames, from which it can determine the frame type, and thus whether the frame is of a type that is generated by a server. If a data frame corresponds to a server frame type, then the source of the data frame must be a server device. Kosbab '808 performs a query "MATCH TO SERVER FRAME TYPE, if there is a match between the frame information and any of the server frame types" (col. 8, lines 16-19) then the server is identified. Since the collected information is being compared to a known set of information associated with the server, Kosbab '808 provides an accurate method of identification.

The Office Action, at page 4, states that there is motivation to modify Kosbab '808 "in order to have a more precise method to identify servers." The Office Action bases a perceived lack of precision on the part of Kosbab '808 on the use of the word "may" in Kosbab '808 at col. 3, lines 5-10 which states:

> The frames being sent may contain information that may be uniquely associated with specific types of network devices such as servers, routers, printers. For example, frames containing router information protocol (RIP) messages may be assumed to be generated by one or more routers. (Emphasis added).

However, Applicants disagree and note that the interpretation of Kosbab '808 use of the word "may" is taken out of context and outside of the dictionary definition of "may." Mariam Webster Dictionary defines may as to "have the ability to" and notes that "may" is "used nearly interchangeably with *can*." From this definition it can be clearly understood that "may" is not imprecise.

Furthermore, Applicants note that the Kosbab '808 specification explains in detail a careful method of determining a device to be a router. The details of Kabob '808 clearly do not support the Office Action interpretation of the word "may" and are reproduced, for convenience, as follows:

> Initially, the node type in the field 132 of the entry 134 may not be known and will typically be set to a default node type, such as "station". The set of network device types includes station, router, server, and printer. Other network device types may be readily added to the set according to the currently available network device types and the need of the user to detect such network device types.
>
> The frames received from the router 24 and other devices on the LAN, including the devices 18, 20, and 22 (shown in FIG. 1) may be unique to one of the set of network device types, including routers, printers, and servers. As frames continue to be received from the router 24, the frame information is compared against a set of router frame types which are unique to routers, further compared to a set of server frame types which are unique to servers, and

then compared to a set of printer frame types which are unique to printers. If there is a match to one of the set of device types, the node type of the field 132 of the entry 134 is filled in with the corresponding network device type.

According to the above example, the router 134 may send a "multicast router information protocol (RIP) reply" which is understood to be unique to routers. The frame information is matched against a corresponding frame type for routers and the device type is entered as "router" in the field 132 of the entry 134. In the same way, the device 22 having an entry 140, which is a file server named "Dilbert" in this example, may be detected when it sends a frame that matches the set of server frame types. The device type "server" is then placed in the field 132 in the entry 140. Because the devices 18 and 20 which have entries 136 and 138 are clients named "Client 1" and "Client 2" respectively, none of their frame types should match those unique to routers, servers, or printers. It is proper that the entries 136 and 138 corresponding to the devices 18 and 20 have their node type in the field 132 remain as "stations" in the station database 104.

The router 24 (shown in FIG. 1) may also be a statically-configured router (static router) which is commonly understood to route network traffic but without affirmatively advertising its presence on the LAN 12. Static routers present a special problem for the test instrument 10 because static routers do not broadcast routing protocols, such as RIP, to share routing information with other routers. Thus, the static router will not generate any of the frame types present in the set of router frame types.

In performing the routing function, the static router, in common with other types of routers, selectively routes frames from network devices con remote networks to the devices on the local network according to a router table. The frames thus relayed have the network address of the remote device along with the MAC address of the router, a property well known in routers. As further frames from network traffic is collected, multiple entries having different network addresses but sharing the same MAC address will appear in the station database 104. If at least four such entries appear, these entries may then be associated with the network device type "route." This is because other network device types such as servers may occasionally have multiple network addresses for one MAC address but will seldom have over two network addresses.

The actual network address among the multiple network addresses collected for the static router is the only entry having a local network address rather than a remote network address. Local addresses are determined by further monitoring of network traffic to determine which frames are uniquely local. For example the ARP (Address Resolution Protocol) request is, according to industry-standard definition, not forwarded by routers and thus contains a network address of a sending network device that is local. Using this local network address for comparison, the local address corresponding to the router may be determined. The present invention thus detects the presence of the static router using an alternative method of using the pattern of stored information within the station database 104 to detect unique patterns associated exclusively with routers.

(col. 5, line 22 to col. 6, line 42, emphasis added; and *noting* the quote presents a method of determining a device to be a router while Kosbab '808 also provides a method of determining a device to be a server at col. 8, lines 21-32, and a method of determining a device to be a printers col. 8, lines 48-52). Applicants respectfully note that clearly Kosbab '808 is not imprecise and there is no support for the Office Action statement that Kosbab '808 provides motivation for Applicants invention. Therefore, Applicants respectfully request that the rejection be withdrawn.

Dieboll '643 and McKee '981 on the other hand describe network management applications that do not receive live data frames, but rather statistical data relating to network traffic, i.e., network management data, previously gathered by probes. Both the probes and the network management application are permanently connected to the network for continuous monitoring. In particular, as in the present invention, Dieboll '643 and McKee '981 receive conversation data containing "source address, destination address, data volume and protocol" information. It is not possible to determine frame types from this static, conversation data, which corresponds to the data used in the present invention, and so it is not possible to implement the technique for identifying servers disclosed in Kosbab '808 in the network management applications disclosed in Dieboll '643 or McKee '981.

Moreover, to implement the method of Kosbab '808 of identifying certain server frame types in the Extract-Servers program of McKee '981 would render much of the Extract-Servers program of McKee '981 redundant. In particular, the description of the Extract-Servers program is for an implementation of network analysis in the case where the traffic data contains no indication of the server/client role of a node sending/receiving data. (see col. 15, lines 3-25). The passage goes on to state that if the node role information is collected, by identifying servers using well known port numbers, then this can be used in identifying the global and local servers instead of carrying out the operation of the Extract-Servers program. The Extract-Servers program is used in the case where traffic does not contain well-known port numbers (i.e., node role information such as used in Kosbab '808), and would not be used if the frame information were available as in Kosbab '808.

In summary, Kosbab '808 and McKee '981/Dieboll '643 relate to quite different methods of determining/distinguishing between server devices in the network. McKee '981 and Dieboll '643 each run on static network management traffic data, whereas Kosbab '808 operates on live packet capture. The level of detail of data available by packet capture is greater then the data which would be stored as network management data (it would not be practical to store more detailed data for network management because of the memory capacity that would be required). However, even if received network management

data contained the same level of detail as is available from packet capture, the network analysis methods of McKee '981 and/or Dieboll '643, to determine or distinguish between servers would be unnecessary. Thus, there is no obvious combination of the features of the prior art documents which would lead the skilled person to the method as defined in claim 1, the corresponding program of claim 16 or the corresponding apparatus of claim 26.

D. Claims 2-16, 17-25 and 27-28

Since claims 2-16, 17-25 and 27-28 depend directly or indirectly from amended independent claims 1, 16 and 26, respectively, based upon the amendments and/or reasons set forth above regarding claims 1, 16 and 26, respectively Applicants respectfully request that the 35 USC § 103 rejections of claims 2-16, 17-25 and 27-28 be withdrawn.

Conclusion

Thus, the Applicants submit that the claims, presently in the application, are not obvious under the provisions of 35 USC § 103.

Consequently, the Applicants believe that all these claims are presently in condition for allowance.

Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,

February 19, 2004

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & ASSOCIATES
formerly Michaelson & Wallace
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **February 20, 2004** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to

Mail Stop Non-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Signature

30,090
Reg. No.

(3COM76AMEND/ca:93)